Política Específica de Controles Criptográficos

ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir las reglas para el uso de los controles y claves criptográficas para proteger la confidencialidad, integridad, autenticidad e inviolabilidad de la información en DACTA.

Este documento se aplica a todo el alcance del Sistema Integrado de Gestión (SIG). Los usuarios de este documento son todos los colaboradores y proveedores de DACTA.

2. DOCUMENTOS DE REFERENCIA

- NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información, clausula 8.24.
- Política Integrada del SIG.
- Política de Gestión de Accesos.

3. POLÍTICA ESPECÍFICA

3.1. De los lineamientos de la política

Dentro de esta política es menester comprender los siguientes términos:

Autenticidad: Propiedad de que una entidad es lo que afirma ser. (Norma ISO 27000:2014, términos y definiciones).

Clave criptográfica: Una clave, palabra clave o clave criptográfica es una pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se
especifica la transformación del texto plano en texto cifrado, o viceversa.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Integridad: La propiedad de salvaguardar la exactitud y complejidad de la información. (Norma ISO27000:2014).

Los controles criptográficos deben usarse siempre que sea necesario para proteger la información confidencial contra el acceso no autorizado. La criptografía es la ciencia de escribir en código secreto, mientras que el cifrado es el mecanismo específico para convertir la información en un código diferente que sea comprensible para quienes conocen el mecanismo de cifrado / descifrado.

Dentro de este contexto DACTA se compromete a:

Garantizar el uso adecuado y eficaz de los mecanismos de criptografía para asegurar la confidencialidad, integridad, autenticidad y no repudio de la información en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada como sensible.
- Para el resguardo de información, cuando así surja de la evaluación de riesgos.
- Protección para firmar documentos electrónicos de la facturación electrónica, que garanticen la autenticidad y no repudio de los mismos.
- Protección en nuestras comunicaciones tanto para colaboradores como usuarios de nuestros servicios.

Establecer los algoritmos de cifrado a utilizar para los distintos escenarios, como parte de nuestros estándares de desarrollo de software y publicación de nuestras aplicaciones:

- Los algoritmos criptográficos que se utilicen en el cifrado de información deben estar definidos por estándares internacionales.
- Las aplicaciones informáticas que transmitan datos por la red deberán contar con un certificado digital para el cifrado de los datos en tránsito.
- La información que sea cifrada por requerimiento del usuario deberá contar con una clave de respaldo administrada por el coordinador TI, para los casos de recuperación.
- Se llevará un control de los certificados digitales en el formato **"F-E-SIG-010 Registro de Control de Certificados digitales"**.
- La fecha de expiración máxima para certificados de firma es como máximo 1 año.
- La fecha de expiración máxima para certificados SSL/TLS es como máximo 2 años.
- Todos los certificados deben tener al menos una longitud de 2048 bits

A aplicar controles criptográficos como mínimo en los siguientes casos:

- SI un dispositivo con información confidencial (disco duro externo, unidad flash, computadora portátil, etc.) sale de la organización.
- Cuando se requiera enviar un correo electrónico con información confidencial.
- Si se tiene un servidor de archivos con una carpeta a la que todos los empleados tienen acceso, pero uno (o más) de los archivos contienen información confidencial.
- Si se tiene un sitio web público al que los usuarios pueden acceder ingresando el nombre de usuario / contraseña (en este caso, la contraseña es información confidencial que, si no viaja por un canal seguro, podría ser revelada).
- Si publicamos un sitio web desde el que ofrecemos comercio electrónico y contamos con una pasarela de pago.
- Sus empleados se conectan a la red corporativa desde casa para acceder a los recursos corporativos.

3.2. De la gestión de las claves

Al desarrollar los sistemas, se deben establecer los algoritmos de cifrado a utilizar para los distintos escenarios.

- Las claves, para acceder a las aplicaciones, deben tener una longitud mínima de 7 caracteres y se debe combinar letras, números y caracteres especiales.
- Las claves deben tener una vigencia luego de la cual el usuario debe verse obligado a cambiarla.
- Las cuentas de usuario y clave son personales e intransferibles. Su uso determina un nivel de responsabilidad por la información que sea manipulada por esta cuenta y clave, por lo tanto, cada usuario asume las consecuencias acciones ejecutadas con esta cuenta de usuario y clave.

En caso de no cumplir con la presente Política Específica, los lineamientos de seguridad de la información u otros directivas o procedimientos de seguridad de la información, se reportará el evento al Comité de Gestión de Seguridad de la Información para que tome conocimiento y disponga las acciones correspondientes, de considerarlo necesario. De esta forma, la autoridad competente del DACTA, tomará las medidas disciplinarias necesarias, las cuales están sujetas al **"M-S-RRHH-002 Código de Ética y Conducta"** de DACTA.

4. REGISTROS

Código	Nombre de Registro	Responsable del Control	Tiempo de Conservación
F-E-SIG-010	Registro de Control de Certificados digitales	OSI	24 meses

5. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaborado por	Revisado por	Aprobado por
1	30/06/2021	Emisión	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
2	22/02/2023	Actualización	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
2	22/02/2024	Revisión	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
Firmas de la versión vigente			 S. Rafaile	 S. Rafaile  A. Morales	 G. Rafaile

Identificación de las modificaciones	
Versión	**Descripción de cambios**
2	Se actualizó el documento con el nuevo logo de DACTA. Se actualiza el requisito normativo según nueva versión ISO 27001:2022.